We claim:

1. A system for enciphering information, comprising:

a first memory access unit configured to retrieve data from a host memory;

a staggered FIFO unit configured to receive the retrieved data from the host memory, the staggered FIFO unit further configured to perform a ShiftRow step of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data;

a second memory access unit configured to receive the produced row-shifted data and perform a byte substitution using the row-shifted data to produce byte-substituted data;

logic configured to receive the byte-substituted data and expand the byte-substituted data to produce manipulated data using a designated expansion algorithm; and

a subprocessor memory configured to receive and store the manipulated data.

2. A system for enciphering information, comprising:

a host processor comprising a host memory, the host memory having data;

a subprocessor having a subprocessor memory, the subprocessor configured to retrieve the data from the host memory and manipulate the data as the data is being loaded into the subprocessor memory.

3. The system of claim 2, wherein the subprocessor is configured to execute an Advanced Encryption Standard (AES) algorithm using the data.

4. The system of claim 3, wherein the subprocessor comprises a first memory access unit configured to retrieve the data from a host memory.

5. The system of claim 4, wherein the subprocessor further comprises a staggered FIFO unit configured to receive the retrieved data from the host memory, the staggered FIFO unit further configured to perform a ShiftRow step of the AES algorithm on the data to produce row-shifted data.

6. The system of claim 5, wherein the subprocessor further comprises a second memory access unit configured to receive the produced row-shifted data and perform a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data.

7. The system of claim 6, wherein the subprocessor further comprises a data expansion unit configured to receive the byte-substituted data and expand the byte-substituted data to produce manipulated data using a designated expansion algorithm.

8. The system of claim 7, wherein the subprocessor further comprises a subprocessor memory configured to receive and store the manipulated data.

9. The system of claim 8, wherein the subprocessor further comprises a subprocessor memory access unit configured to retrieve the stored data.

10. The system of claim 5, wherein the staggered FIFO unit comprises:

a first set of variable-layer FIFOs having a plurality of FIFO layers, the first set of variable-layer FIFOs configured to receive a first portion of the data in response to a designated clock signal, the first set of variable-layer FIFOs further configured to cascade the received first portion of the data through the plurality of FIFO layers in response to consecutive clock signals after the designated clock signal, the variable-layer FIFOs further configured to release the cascaded first portion of the data; and

a second set of variable-layer FIFOs having a plurality of FIFO layers, the second set of variable-layer FIFOs configured to receive a second portion of the data in response to the designated clock signal, the second set of variable-layer FIFOs further configured to cascade the received second portion of the data through the plurality of FIFO layers in response to the consecutive clock signals after the designated clock signal, the second set of variable-layer FIFOs further configured to buffer the cascaded second portion of the data for one clock cycle, the variable-layer FIFOs further configured to release the buffered second portion of the data.

11. The system of claim 10, wherein the data comprises a matrix having four rows of data, each of the four rows of data having four bytes of data.

12. The system of claim 11, wherein the first set of variable-layer FIFOs comprises a first release-FIFO layer configured to receive a first set of three bytes of the data matrix in response to a designated clock signal, the first release-FIFO layer further configured to release the first set of three bytes of the data matrix in response to a first clock signal, the first clock signal immediately following the designated clock signal, the first release-FIFO layer further

configured to receive a second set of three bytes of the data matrix in response to the first clock signal, the first release-FIFO layer further configured to release the second set of three bytes of the data matrix in response to a second clock signal, the second clock signal immediately following the first clock signal, the first release-FIFO layer further configured to receive a third set of three bytes in response to the second clock signal, the first release-FIFO layer further configured to release the third set of three bytes in response to a third clock signal, the third clock signal immediately following the second clock signal, the first release-FIFO layer further configured to receive a fourth set of three bytes in response to the third clock signal, the first release-FIFO layer further configured to release the fourth set of three bytes in response to a fourth clock signal, the fourth clock signal immediately following the third clock signal.

13. The system of claim 12, wherein the first set of variable-layer FIFOs further comprises a second release-FIFO layer configured to receive two bytes of the first set of three bytes in response to the first clock signal, the second release-FIFO layer further configured to release the two bytes of the first set of three bytes in response to the second clock signal, the second release-FIFO layer further configured to receive two bytes of the second set of three bytes in response to the second clock signal, the second release-FIFO layer further configured to release the two bytes of the second set of three bytes in response to the third clock signal, the second release-FIFO layer further configured to receive two bytes of the third set of three bytes in response to the third clock signal, the second release-FIFO layer further configured to release the two bytes of the third set of three bytes in response to the fourth clock signal, the second release-FIFO layer further configured to receive two bytes of the fourth set of three bytes in response to the fourth clock signal, the second release-FIFO layer further configured to release

the two bytes of the fourth set of three bytes in response to a fifth clock signal, the fifth clock signal immediately following the fourth clock signal.

14. The system of claim 13, wherein the first set of variable-layer FIFOs further comprises a third release-FIFO layer configured to receive one byte of the two bytes of the first set of three bytes in response to the second clock signal, the third release-FIFO layer further configured to release the one byte of the two bytes of the first set of three bytes in response to the third clock signal, the third release-FIFO layer further configured to receive one byte of the two bytes of the second set of three bytes in response to the third clock signal, the third release-FIFO layer further configured to release the one byte of the two bytes of the second set of three bytes in response to the fourth clock signal, the third release-FIFO layer further configured to receive one byte of the two bytes of the third set of three bytes in response to the fourth clock signal, the third release-FIFO layer further configured to release the one byte of the two bytes of the third set of three bytes in response to the fifth clock signal, the third release-FIFO layer further configured to receive one byte of the two bytes of the fourth set of three bytes in response to the fifth clock signal, the third release-FIFO layer further configured to release the one byte of the two bytes of the fourth set of three bytes in response to a sixth clock signal, the sixth clock signal immediately following the fifth clock signal.

15. The system of claim 14, wherein the second set of variable-layer FIFOs comprises a first delay-FIFO layer configured to receive a second set of one byte of the data matrix in response to the first clock signal, the first delay-FIFO layer further configured to release the second set of one byte of the data matrix in response to the second clock signal, the first delay-

FIFO layer further configured to receive a third set of one byte of the data matrix in response to the second clock signal, the first delay-FIFO layer further configured to release the third set of one byte of the data matrix in response to the third clock signal, the first delay-FIFO layer further configured to receive a fourth set of one byte in response to the third clock signal, the first delay-FIFO layer further configured to hold the fourth set of one byte in response to a fourth clock signal, the first delay-FIFO layer further configured to release the fourth set of one byte in response to the fifth clock signal.

16. The system of claim 15, wherein the second set of variable-layer FIFOs further comprises a second delay-FIFO layer configured to receive, in response to the second clock signal, the second set of one byte of the data matrix and one byte of the first set of three bytes from the first release-FIFO layer, the second delay-FIFO layer further configured to release, in response to the third clock signal, the second set of one byte of the data matrix and the one byte of the first set of three bytes from the first release-FIFO layer, the second delay-FIFO layer further configured to receive, in response to the third clock signal, the third set of one byte of the data matrix and one byte of the second set of three bytes from the first release-FIFO layer, the second delay-FIFO layer further configured to hold, in response to the fourth clock signal, the third set of one byte of the data matrix and the one byte of the second set of three bytes from the first release-FIFO layer, the second delay-FIFO layer further configured to release, in response to the fifth clock signal, the third set of one byte of the data matrix and the one byte of the second set of three bytes from the first release-FIFO layer, the second delay-FIFO layer further configured to receive, in response to the fifth clock signal, the fourth set of one byte of the data matrix and one byte of the third set of three bytes from the first release-FIFO layer, the second

delay-FIFO layer further configured to release, in response to the sixth clock signal, the fourth set of one byte of the data matrix and the one byte of the third set of three bytes from the first release-FIFO layer.

17. The system of claim 16, wherein the second set of variable-layer FIFOs further comprises a third delay-FIFO layer configured to receive, in response to the third clock signal, the second set of one byte of the data matrix and two bytes of the first set of three bytes from the first release-FIFO layer, the third delay-FIFO layer further configured to hold, in response to the fourth clock signal, the second set of one byte of the data matrix and the two bytes of the first set of three bytes from the first release-FIFO layer, the third delay-FIFO layer further configured to release, in response to the fifth clock signal, the second set of one byte of the data matrix and the two bytes of the first set of three bytes from the first release-FIFO layer, the third delay-FIFO layer further configured to receive, in response to the fifth clock signal, the third set of one byte of the data matrix and two bytes of the second set of three bytes from the first release-FIFO layer, the third delay-FIFO layer further configured to release, in response to the sixth clock signal, the third set of one byte of the data matrix and the two bytes of the second set of three bytes from the first release-FIFO layer, the third delay-FIFO layer further configured to output, in response to the sixth clock signal, the fourth set of one byte of the data matrix and the two bytes of the third set of three bytes from the first release-FIFO layer.

18. The system of claim 6, wherein the substitution table is located in the host memory.

19. The system of claim 6, wherein the substitution table is configured as a hardware logic component within the subprocessor.

20. The system of claim 6, wherein the substitution table is located in the subprocessor memory.

21. A system for enciphering information, comprising:

means for retrieving data from a host memory;

means for performing a ShiftRow operation of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data;

means for performing a byte substitution using the row-shifted data to produce byte-substituted data;

means for expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm; and

means for storing the manipulated data.

22. A system for enciphering information, comprising:

means for retrieving data from the host memory; and

means for manipulating the data as the data is being loaded into a subprocessor memory.

23. The system of claim 22, wherein the means for manipulating the data further comprises means for executing an Advanced Encryption Standard (AES) algorithm using the data.

24. The system of claim 23, wherein the means for executing the AES algorithm further comprises means for retrieving data from a host memory.

25. The system of claim 24, further comprising means for performing a ShiftRow step of the AES algorithm on the data to produce row-shifted data.

26. The system of claim 25, further comprising means for performing a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data.

27. The system of claim 26, further comprising means for expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm.

28. The system of claim 27, further comprising means for storing the manipulated data.

29. The system of claim 28, further comprising means for retrieving the stored data.

30. The system of claim 25, wherein the means for performing the ShiftRow step further comprises:

means for receiving a portion of the data in response to a designated clock signal;

means for cascading the received portion of the data through a first set of FIFOs in response to consecutive clock signals after the designated clock signal;

means for releasing the cascaded portion of the data;

means for receiving a remaining portion of the data in response to the designated clock signal;

means for cascading the received remaining portion of the data through a second set of FIFOs in response to the consecutive clock signals after the designated clock signal;

means for buffering the cascaded remaining portion of the data for one clock cycle; and

means for releasing the buffered remaining portion of the data.

31. A method for enciphering information, comprising the steps of:

retrieving data from a host memory;

performing a ShiftRow operation of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data;

performing a byte substitution using the row-shifted data to produce byte-substituted data;

expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm; and

storing the manipulated data.

32. A method for enciphering information, comprising the steps of:

retrieving data from the host memory; and

manipulating the data as the data is being loaded into a subprocessor memory.

33. The method of claim 32, wherein the step of manipulating the data comprises the step of executing the Advanced Encryption Standard (AES) algorithm using the data.

34. The method of claim 33, wherein the step of executing the AES algorithm comprises the step of performing a ShiftRow step of the AES algorithm on the data to produce row-shifted data.

35. The method of claim 34, further comprising the step of performing a byte substitution operation on the row-shifted data using a substitution table to produce byte-substituted data.

36. The method of claim 35, further comprising the step of expanding the byte-substituted data to produce manipulated data using a designated expansion algorithm.

37. The method of claim 36, further comprising the step of storing the manipulated data in subprocessor memory.

38. The method of claim 37, further comprising the step of retrieving the data stored in subprocessor memory.

39. The method of claim 34, wherein the step of performing the ShiftRow operation further comprises:

receiving a first portion of the data in response to a designated clock signal;

cascading the received first portion of the data through a first set of FIFOs in response to consecutive clock signals after the designated clock signal;

releasing the cascaded first portion of the data;

receiving a second portion of the data in response to the designated clock signal;

cascading the received second portion of the data through a second set of FIFOs in response to the consecutive clock signals after the designated clock signal;

buffering the cascaded second portion of the data for one clock cycle; and

releasing the buffered second portion of the data.

40. The method of claim 39, further comprising the step of arranging the data into a matrix having four rows, each of the four rows having four bytes.

41. The method of claim 40, wherein the step of cascading the received first portion of the data through the first set of FIFOs comprises the steps of:

receiving a first set of three bytes of the data matrix in response to a designated clock signal;

releasing the first set of three bytes of the data matrix in response to a first clock signal, the first clock signal immediately following the designated clock signal;

receiving a second set of three bytes of the data matrix in response to the first clock signal;

releasing the second set of three bytes of the data matrix in response to a second clock signal, the second clock signal immediately following the first clock signal;

receiving a third set of three bytes in response to the second clock signal;

releasing the third set of three bytes in response to a third clock signal, the third clock signal immediately following the second clock signal;

receiving a fourth set of three bytes in response to the third clock signal; and

releasing the fourth set of three bytes in response to a fourth clock signal, the fourth clock signal immediately following the third clock signal.

42. The method of claim 41, wherein the step of cascading the received first portion of the data through the first set of FIFOs further comprises the steps of:

receiving two bytes of the first set of three bytes in response to the first clock signal;

releasing the two bytes of the first set of three bytes in response to the second clock signal;

receiving two bytes of the second set of three bytes in response to the second clock signal;

releasing the two bytes of the second set of three bytes in response to the third clock signal;

receiving two bytes of the third set of three bytes in response to the third clock signal;

releasing the two bytes of the third set of three bytes in response to the fourth clock signal;

receiving two bytes of the fourth set of three bytes in response to the fourth clock signal; and

releasing the two bytes of the fourth set of three bytes in response to a fifth clock signal, the fifth clock signal immediately following the fourth clock signal.

43. The method of claim 42, wherein the step of cascading the received first portion of the data through the first set of FIFOs further comprises the steps of:

receiving one byte of the two bytes of the first set of three bytes in response to the second clock signal;

releasing the one byte of the two bytes of the first set of three bytes in response to the third clock signal;

receiving one byte of the two bytes of the second set of three bytes in response to the third clock signal;

releasing the one byte of the two bytes of the second set of three bytes in response to the fourth clock signal;

receiving one byte of the two bytes of the third set of three bytes in response to the fourth clock signal;

releasing the one byte of the two bytes of the third set of three bytes in response to the fifth clock signal;

receiving one byte of the two bytes of the fourth set of three bytes in response to the fifth clock signal; and

releasing the one byte of the two bytes of the fourth set of three bytes in response to a sixth clock signal, the sixth clock signal immediately following the fifth clock signal.

44. The method of claim 43, wherein the step of cascading the received second portion of the data through the second set of FIFOs comprises the steps of:

receiving a second set of one byte of the data matrix in response to the first clock signal;

releasing the second set of one byte of the data matrix in response to the second clock signal;

receiving a third set of one byte of the data matrix in response to the second clock signal;

releasing the third set of one byte of the data matrix in response to the third clock signal;

receiving a fourth set of one byte in response to the third clock signal;

holding the fourth set of one byte in response to the fourth clock signal; and

releasing the fourth set of one byte in response to the fifth clock signal.

45. The method of claim 44, wherein the step of cascading the received second portion of the data through the second set of FIFOs further comprises the steps of:

receiving, in response to the second clock signal, the second set of one byte of the data matrix and one byte of the first set of three bytes;

releasing, in response to the third clock signal, the second set of one byte of the data matrix and the one byte of the first set of three bytes;

receiving, in response to the third clock signal, the third set of one byte of the data matrix and one byte of the second set of three bytes;

holding, in response to the fourth clock signal, the third set of one byte of the data matrix and the one byte of the second set of three bytes;

releasing, in response to the fifth clock signal, the third set of one byte of the data matrix and the one byte of the second set of three bytes;

receiving, in response to the fifth clock signal, the fourth set of one byte of the data matrix and one byte of the third set of three bytes; and

releasing, in response to the sixth clock signal, the fourth set of one byte of the data matrix and the one byte of the third set of three bytes .

46. The method of claim 45, wherein the step of cascading the received second portion of the data through the second set of FIFOs further comprises the steps of:

receiving, in response to the third clock signal, the second set of one byte of the data matrix and two bytes of the first set of three bytes;

holding, in response to the fourth clock signal, the second set of one byte of the data matrix and two bytes of the first set of three bytes;

releasing, in response to the fifth clock signal, the second set of one byte of the data matrix and two bytes of the first set of three bytes;

receiving, in response to the fifth clock signal, the third set of one byte of the data matrix and two bytes of the second set of three bytes;

releasing, in response to the sixth clock signal, the third set of one byte of the data matrix and two bytes of the second set of three bytes; and

output, in response to the sixth clock signal, the fourth set of one byte of the data matrix and two bytes of the third set of three bytes .

47. The method of claim 35, wherein the step of performing the byte substitution operation further comprises the step of accessing a substitution table located in the host memory.

48. The method of claim 35, wherein the step of performing the byte substitution operation further comprises the step of accessing a substitution table configured as a hardware logic component within the subprocessor.

49. The method of claim 35, wherein the step of performing the byte substitution operation further comprises the step of accessing a substitution table located in the subprocessor memory.